U.S. Department of Justice

United States Attorney
Eastern District of New York

SDD:DMP
F.#2013R01131

271 Cadman Plaza East
Brooklyn, New York 11201

January 31, 2017

By Hand Delivery and ECF

The Honorable Kiyo A. Matsumoto
United States District Court
Eastern District of New York
225 Cadman Plaza East
Brooklyn, NY 11201

Re: United States v. Ercan Findikoglu
Criminal Docket No. 13-440 (KAM)

Dear Judge Matsumoto:

The government respectfully submits this letter in anticipation of the February 7, 2017 sentencing of Ercan Findikoglu, a Turkish citizen also known by the online nicknames "Segate," "Predator," and "Oreon." Findikoglu was one of the masterminds behind three cyberattacks between 2011 and 2013 that inflicted more than $55 million in losses on the global financial system. For the reasons stated below, the government respectfully requests that the Court sentence the defendant to a term of imprisonment within the advisory United States Sentencing Guidelines ("U.S.S.G." or the "Guidelines") range of 135 to 168 months.

I. Offense Conduct

As described in the Pre-Sentence Investigation Report ("PSR") and in the stipulated facts to which the defendant agreed as part of his guilty plea, Findikoglu organized three worldwide cyberattacks known in the cyber underworld as "Unlimited Operations" or "cashouts." Such cyberattacks have several phases:

- First, the hackers plan and execute sophisticated cyber intrusions to gain unauthorized access to the computer networks of credit card processors that are responsible for processing prepaid debit card transactions. They target databases of prepaid debit cards, which are typically loaded with finite funds; such cards are used by, for example, many employers in lieu of paychecks and by charitable organizations to distribute disaster assistance. The cybercriminals bypass or breach the

security protocols on the debit card accounts and then dramatically increase the balances and effectively eliminate the withdrawal limits on the accounts. The elimination of withdrawal limits enables the participants to withdraw literally unlimited amounts of cash until the operation is shut down, hence the name "Unlimited Operation."

- Next, the cybercrime organization cashes in, by distributing the hacked prepaid debit card numbers to trusted associates around the world. These associates operate cells or teams of "cashers," who encode magnetic stripe cards, such as gift cards, with the compromised debit card account data. When the cybercrime organization distributes the personal identification numbers ("PINs") for the hacked accounts, the casher cells spring into action, using these "debit cards" and PINs to immediately withdraw cash from ATMs across the globe. Meanwhile, the cybercrime organization maintains access to the computer networks of the credit card processors they have hacked in order to monitor the withdrawals.

- Finally, at the end of an operation, when the cards are shut down, the casher cells launder the proceeds, often investing the operation's proceeds in luxury goods, and kick money back up to the cybercrime organization's leaders.

Unlimited Operations are marked by three key characteristics: (1) the surgical precision of the hackers carrying out the cyberattack; (2) the global nature of the cybercrime organization; and (3) the speed and coordination with which the organization executes its operations on the ground. These attacks rely upon both highly sophisticated hackers, as well as organized criminal cells whose role is to withdraw the cash as quickly as possible.

Findikoglu was one of the principal leaders and organizers of three Unlimited Operations:

A. The FIS Unlimited Operation

The first operation, on February 27 and 28, 2011, targeted a credit and debit card payment processor called Fidelity National Information Services, Inc. ("FIS"), which was based in Florida. Between December 2010 and February 2011, Findikoglu penetrated FIS's computer network, gained unauthorized access to an FIS prepaid debit card database, breached security protocols and increased the withdrawal limits on 21 prepaid cards issued by JPMorgan Chase. Notably, these prepaid cards were used by the American Red Cross to provide charitable relief funds to victims of natural disasters.

Findikoglu and his co-conspirators distributed the data for these prepaid cards to other co-conspirators around the world who encoded the account information onto plastic

cards with magnetic strips. Findikoglu instructed these co-conspirators to gather crews of cashers who could withdraw money at an appointed time. When the crews were assembled, Findikoglu distributed the PIN numbers via text message to the leaders of the cashing crews.

On February 27 and 28, 2011, the compromised FIS prepaid cards were used in approximately 15,000 transactions in 18 countries, resulting in approximately $10 million in fraudulent withdrawals, including in Brooklyn, New York.

Findikoglu had access to the FIS network database and watched in real-time as the money was withdrawn. He could tell if the compromised FIS prepaid cards were being used somewhere he had not authorized their use and could shut them off.

Following this operation, Findikoglu and his co-conspirators received a delivery of approximately $300,000 in proceeds from one of the mangers of a cashing crew who traveled to Turkey to deliver the money. Findikoglu also received other proceeds by wire transfer and other means.

B. The ECS/RAKBANK Unlimited Operation

The second of these Unlimited Operations targeted ElectraCard Services ("ECS"), a payment processor based in India. In December 2012, ECS was the victim of a network intrusion. As a result, Findikoglu and his co-conspirators were able to obtain unauthorized access to an ECS prepaid debit card database, among other things. They breached security protocols and increased withdrawal limits on prepaid cards issued by the National Bank of Ras Al-Khaimah PSC, also known as "RAKBANK," located in the United Arab Emirates. Findikoglu and his co-conspirators distributed the data for the compromised ECS cards to leaders of the cashing crews around the world.

On December 21 and 22, 2012, the compromised ECS cards were used in approximately 5,000 transactions in 20 countries, resulting in approximately $5 million in fraudulent withdrawals. In New York alone, cashers conducted more than 700 fraudulent withdrawals, totaling nearly $400,000 in losses, at more than 140 different ATM locations over the course of just two and a half hours.

At Findikoglu's direction, cash proceeds from fraudulent withdrawals made in New York in the course of the ECS/RAKBANK Unlimited Operation were transported from Queens, New York to co-conspirators in Romania by New York-based cashers who participated in the operation. Findikoglu received proceeds of this Unlimited Operation by wire transfer and other means.

C. The enStage/Bank Muscat Unlimited Operation

The third Unlimited Operation occurred on the afternoon of February 19, 2013 and lasted into the early morning of February 20, 2013. In this operation, Findikoglu and his co-conspirators breached the network of a credit card processor called enStage, which was

based in California. They breached security protocols and increased withdrawal limits on MasterCard prepaid debit cards issued by Bank Muscat, located in Oman.

Findikoglu and his co-conspirators distributed the data for the compromised enStage cards to the leaders of cashing crews around the world. On February 19 and 20, 2013, these compromised cards were used in a particularly devastating cyberattack. Over the course of approximately 10 hours, casher cells in 24 countries executed approximately 36,000 transactions and withdrew approximately $40 million in fraudulent transactions. From 3 p.m. on February 19 through 1:26 a.m. on February 20, cashers withdrew approximately $2.4 million in nearly 3,000 ATM withdrawals in the New York City area alone.

Following this operation, Findikoglu and his co-conspirators again received a delivery of cash in Turkey from one of the mangers of a cashing crew as well as additional proceeds by wire transfer.

On March 1, 2016, Findikoglu pleaded guilty to computer intrusion conspiracy, in violation of Title 18, United States Code, Section 371, and conspiracy to commit access device fraud, in violation of Title 18, United States Code, Section 1029(b)(2), for his role in these Unlimited Operations between January 2010 and July 2013. Findikoglu also pleaded guilty to three counts of access device fraud, in violation of Title 18, United States Code, Section 1029(a)(5), for his role in each of three Unlimited Operations described above.

II. The Guidelines Calculation

The government agrees with the Guidelines calculation set forth in the PSR. Specifically, the total offense level is 36, based on a base offense level of 6, a 22-level enhancement for a loss amount of approximately $55 million, a two-level enhancement because a substantial part of the fraud was committed outside the United States, a two-level enhancement for the use of device-making equipment, a four-level leadership role enhancement, and a three-level reduction for acceptance of responsibility. With a criminal history category of I, the resulting advisory Guidelines range of imprisonment is 135 to 168 months. The government notes that, in connection with his guilty plea, the defendant stipulated to this Guidelines calculation.

III. Applicable Law

It is settled law that "a district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range. As a matter of administration and to secure nationwide consistency, the Guidelines should be the starting point and the initial benchmark." Gall v. United States, 552 U.S. 38, 49 (2007) (citation omitted). Next, a sentencing court should "consider all of the § 3553(a) factors to determine whether they support the sentence requested by a party. In so doing, [it] may not presume that the

Guidelines range is reasonable. [It] must make an individualized assessment based on the facts presented." Id. at 50 (citation and footnote omitted).

Title 18, United States Code, Section 3553(a) provides that, in imposing sentence, the Court shall consider:

> (1) the nature and circumstances of the offense and the history and characteristics of the defendant;
>
> (2) the need for the sentence imposed –
>
> > (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
> >
> > (B) to afford adequate deterrence to criminal conduct; [and]
> >
> > (C) to protect the public from further crimes of the defendant.

Section 3553 also addresses the need for the sentence imposed "to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner." 18 U.S.C. § 3553(a)(2)(D). "[I]n determining whether to impose a term of imprisonment, and, if a term of imprisonment is to be imposed, in determining the length of the term, [the Court] shall consider the factors set forth in section 3553(a) to the extent that they are applicable, recognizing that imprisonment is not an appropriate means of promoting correction and rehabilitation." 18 U.S.C. § 3582(a).

It is well settled that, at sentencing, "the court is virtually unfettered with respect to the information it may consider." United States v. Alexander, 860 F.2d 508, 513 (2d Cir. 1988). Indeed, Title 18, United States Code, Section 3661 expressly provides that "[n]o limitation shall be placed on the information concerning the background, character, and conduct of a person convicted of an offense which a court of the United States may receive and consider for the purpose of imposing an appropriate sentence." Thus, the Court must first calculate the correct Guidelines range, and then apply the 3553(a) factors to arrive at an appropriate sentence, considering all relevant facts.

IV. Discussion

The government respectfully submits that a sentence within the advisory Guidelines range of 135 to 168 months' imprisonment is appropriate. The Guidelines range reflects the seriousness of the defendant's conduct, the need to promote respect for the law and to impose just punishment, and the need to provide adequate deterrence to the defendant and to others contemplating similar acts. See 18 U.S.C. § 3553(a)(1), (a)(2)(A), (a)(2)(B).

As noted above, Findikoglu was one of the masterminds behind three significant cash-out operations that wreaked havoc with the worldwide financial system by causing losses of more than $55 million. Findikoglu was a skilled hacker who, rather than using his talents for legitimate pursuits, instead put them to work for criminal financial gain.

He and his co-conspirators used their computer skills to hack into the databases of three payment processors, obtain network administrator privileges in these databases and manipulate account balances within these databases. Through online carding forums devoted to access device fraud, Findikoglu and his co-conspirators recruited a huge network of managers and workers ready to spring into action and conduct ATM cash-outs once Findikoglu and the other leaders gave the word. Findikoglu and his co-conspirators maintained complete control during each of these cash-out operations, monitoring them in real-time through their access to the databases of the victim processing companies and shutting off cash-outs in locations that they had not authorized. Indeed, Findikoglu and his co-conspirators sent transaction logs that they obtained from their real-time monitoring to the managers of the cashing crews in order to show how much money had been withdrawn, and accordingly, how much money they were owed. Findikoglu personally received a significant portion of the illegal proceeds from these Unlimited Operations. In short, operating from the perceived safety and anonymity of their computers, Findikoglu and his co-conspirators stole millions of dollars from innocent victims.

In his sentencing memorandum, the defendant argues for a below-Guidelines sentence in light of his personal history and family circumstances, a pending sentencing judgment against him in Turkey, and sentences which this Court has imposed on other co-defendants. As to the first of these arguments, the Probation Department agreed that a variance – though not a downward departure from the Guidelines range – might be appropriate because the defendant will be unable to see his family while incarcerated in the United States and does not know anyone else in the United States. The government has no objection to the Court's consideration of this factor at sentencing. However, the government disagrees that the other two arguments the defendant raises warrant any mitigation of his sentence.

With respect to the pending sentence in Turkey, there is no dispute that in 2008, prior to the commission of the instant offenses for which Findikoglu is being sentenced, he was arrested and convicted in Turkey for participating in a conspiracy to produce fake debit and credit cards. He has served 23 months of a 19½-year sentence that has since been affirmed on appeal. Findikoglu requests that the Court take into account that after he completes a term of imprisonment in the United States, he will be deported to Turkey, where he will have to serve out the remainder of that sentence.

In the government's view, Findikoglu's prior crime in Turkey represents an aggravating, rather than a mitigating, factor. Findikoglu conspired to commit credit card fraud in Turkey, a similar activity for which he has been convicted in this case. Findikoglu's arrest and conviction preceded his involvement in this case, but that conviction did not prevent him from spending the next four years continuing to commit essentially the same types of crimes. The Sentencing Guidelines do not consider foreign convictions in determining a defendant's criminal history category. See U.S.S.G. § 4A1.1 App. Note 3. Nevertheless, the Guidelines provide that a court may consider a foreign conviction in determining whether the defendant's criminal history category underrepresents the seriousness of the defendant's criminal history. See U.S.S.G. § 4A1.2(h) ("Sentences

resulting from foreign convictions are not counted, but may be considered under § 4A1.3 (Adequacy of Criminal History Category)"). Section 4A1.3 provides, in turn, that prior sentences not used in computing the criminal history category, such as foreign sentences, may form the basis for an upward departure. See U.S.S.G. § 4A1.3(a)(2)(A). Numerous Second Circuit cases have upheld a district court's discretion to use a foreign conviction to increase a sentence within a Guidelines range or to upwardly depart from that Guidelines range. See, e.g., United States v. Guzman-Betancourt, 456 Fed. Appx. 64, 67 (2d Cir. 2012), as amended (Mar. 7, 2012) (summary order) (upward departure); United States v. Simmons, 343 F.3d 72, 78 (2d Cir. 2003) (upward departure); United States v. Azeem, 946 F.2d 13, 18 (2d Cir. 1991) (increased sentence within Guidelines range); United States v. Soliman, 889 F.2d 441, 444-45 (2d Cir. 1989) (increased sentence within Guidelines range).

Here, consistent with the terms of the plea agreement, the government is not seeking an upward departure based on Findikoglu's criminal history category being underrepresented. But, at the same time, the government does not believe it is appropriate to reduce Findikoglu's sentence for the instant offense based on the fact that he still has time left to serve on his foreign conviction. Indeed, there is no guarantee that Findikoglu will ever be required to serve a 19½ year sentence. As noted in Findikoglu's sentencing submission, Turkey has instituted a program in which non-violent prisoners who serve half their sentences could be released early on parole. Other changes to Turkey's criminal justice system may likewise mean that Findikoglu would not serve such a sentence upon his return to Turkey.

The defendant also seeks a below-Guidelines sentence in light of below-Guidelines sentences imposed by this Court in cases involving co-conspirators. However, the government submits that Findikoglu is not comparable to these co-conspirators. For the most part, the co-conspirators referred to in his sentencing submission are low-level cashers who were part of the New York cashing crew for the Unlimited Operations.[1] These low-level cashers were primarily young men and women from impoverished circumstances who spent a few hours cashing fraudulent cards at ATMs in exchange for several hundred dollars. They faced significant sentencing ranges under the Sentencing Guidelines because they were held accountable for the entire amount cashed by the New York crew for the Unlimited Operations in which they participated. In a number of instances, the Court gave those low-level cashers below-Guidelines sentences because of those defendants' personal circumstances and because the amounts for which each defendant was accountable was far greater than the limited amounts that each individual defendant personally cashed during the Unlimited Operations.

Finidkoglu, in contrast, was a leader of these Unlimited Operations. He had a proprietary interest in all of the money that was withdrawn, and in fact, monitored the cash-outs in real-time so that he could shut off withdrawals in locations that he had not authorized.

[1] The leader of this crew, Alberto Lajud-Pena, was killed in the Dominican Republic and therefore never appeared before this Court.

He received hundreds of thousands of dollars in payments for his role in obtaining and distributing the card numbers and PINs for the cash-outs. As a result, the government respectfully submits that the approach taken by the Court with respect to the other co-conspirators is not appropriate for someone who was one of the masterminds of the overall fraudulent scheme and who exercised control over nearly every aspect of that scheme.

V. Restitution and Forfeiture

As part of his plea agreement, Findikoglu consented to the entry of a forfeiture money judgment in the amount of $55,080,226.14 as well as forfeiture of approximately 14,000 Euros seized on or about June 23, 2015. On March 1, 2016, this Court entered a preliminary order of forfeiture concerning this money judgment and seized currency. At the time of sentencing, the government will provide the Court with a final order of forfeiture. The government respectfully requests that the Court orally pronounce the forfeiture judgment and attach the final order of forfeiture to the judgment of conviction. The government notes that on March 1, 2016, the defendant paid $10,000 toward the forfeiture money judgment.

In addition, restitution in the amount of $55,080,226.14 is mandatory, pursuant to Title 18, United States Code, Sections 3663A and 3664. The government respectfully requests that the Court order restitution to the victims of the defendant's criminal activity as set forth in the PSR. (See PSR ¶ 78).

VI. Conclusion

For the foregoing reasons, the government respectfully submits that a sentence within the advisory Guidelines range of 135 to 168 months' imprisonment is appropriate.

Respectfully submitted,

ROBERT L. CAPERS
United States Attorney

By: /s/ Douglas M. Pravda
Douglas M. Pravda
Richard M. Tucker
Saritha Komatireddy
Assistant U.S. Attorneys
(718) 254-7000

cc: Clerk of Court (KAM) (by ECF)
Christopher Madiou, Esq. (by ECF)
Jennifer Fisher, United States Probation Officer (by email)